On a conjecture of Schnoebelen

Antonio Cano Gómez, Jean-Eric Pin

On a conjecture of Schnoebelen.

Antonio Cano Gómez* and Jean-Éric Pin†

Jean-Eric.Pin@liafa.jussieu.fr, acano@dsic.upv.es

Abstract

The notion of sequential and parallel decomposition of a language over a set of languages was introduced by Schnoebelen. A language is decomposable if it belongs to a finite set of languages $\mathcal{S}$ such that each member of $\mathcal{S}$ admits a sequential and parallel decomposition over $\mathcal{S}$. We disprove a conjecture of Schnoebelen concerning decomposable languages and establish some new properties of these languages.

1 Introduction

The shuffle product is a standard tool for modeling process algebras [1]. This motivates the study of "robust" classes of recognizable languages which are closed under shuffle product. By "robust" classes, we mean classes which are closed under standard operations, like boolean operations, morphims or inverse morphisms, etc. For instance, a complete classification is known for varieties of languages.

2 Preliminaries

We assume that the reader has a basic background in formal language theory.

2.1 Rational and recognizable sets

Let M be a monoid. A subset P of M is *recognizable* if there exists a finite monoid F, and a monoid morphism $\varphi : M \to F$ such that $P = \varphi^{-1}(\varphi(P))$. It is well known that the class $\mathrm{Rec}(M)$ of recognizable subsets of M is closed under finite union, finite intersection and complement.

The class $\mathrm{Rat}(M)$ of *rational* subsets of M is the smallest set $\mathcal{R}$ of subsets of M satisfying the following properties:

(1) For each $m \in M$, $\{m\} \in \mathcal{R}$

(2) The empty set belongs to $\mathcal{R}$, and if X, Y are in $\mathcal{R}$, then $X \cup Y$ and XY are also in $\mathcal{R}$.

*Departamento de Sistemas Informáticos y Computación, Universidad Politénica de Valencia, Camino de Vera s/n, P.O. Box: 22012, E-46020 - Valencia.

†LIAFA, Université Paris VII and CNRS, Case 7014, 2 Place Jussieu, 75251 Paris Cedex 05, France. Work supported by INTAS project 1224.

(3) If $X \in \mathcal{R}$, the submonoid X^* generated by X is also in $\mathcal{R}$.

Let us briefly remind some important results about recognizable and rational sets.

Theorem 2.1 (Kleene) *For every finite alphabet A,* $\mathrm{Rec}(A^*) = \mathrm{Rat}(A^*)$.

Proposition 2.2 *Let M be a monoid. Then* $\mathrm{Rec}(M)$ *is closed under boolean operations and left and right quotients. Furthermore, if φ is a monoid morphism from M into N, $X \in \mathrm{Rec}(N)$ implies $\varphi^{-1}(X) \in \mathrm{Rec}(M)$.*

In other words, recognizable sets are closed under boolean operations, quotients and inverse morphisms.

Proposition 2.3 *Let M be a monoid. Then* $\mathrm{Rat}(M)$ *is closed under finite union, finite product and star. Furthermore, if φ is a monoid morphism from M into N, $X \in \mathrm{Rat}(M)$ implies $\varphi(X) \in \mathrm{Rat}(N)$.*

In other words, rational sets are closed under rational operations (union, product and star) and under morphisms.

Theorem 2.4 (McKnight) *The intersection of a rational set and of a recognizable set is rational.*

Theorem 2.5 (Mezei) *Let $M_1, \ldots, M_n$ be monoids. A subset of $M_1 \times \cdots \times M_n$ is recognizable if and only if it is a finite union of subsets of the form $R_1 \times \cdots \times R_n$, where $R_i \in \mathrm{Rec}(M_i)$.*

Proposition 2.6 *Let $A_1, \ldots, A_n$ be finite alphabets. Then* $\mathrm{Rec}(A_1^* \times A_2^* \times \cdots \times A_n^*)$ *is closed under product.*

A *substitution* from A^* into a monoid M is a monoid morphism from A^* into $\mathcal{P}(M)$.

3 Decompositions of languages

Consider the transductions τ and σ from A^* into $A^* \times A^*$ defined as follows:

$$\tau(w) = \{(u, v) \in A^* \times A^* \mid w = uv\}$$
$$\sigma(w) = \{(u, v) \in A^* \times A^* \mid w \in u \mathbin{\text{Ш}} v\}$$

Proposition 3.1 *The transduction σ is a substitution.*

Proof. We claim that $\sigma(x_1x_2) = \sigma(x_1)\sigma(x_2)$. First, if $(u_1, v_1) \in \sigma(x_1)$ and $(u_2, v_2) \in \sigma(x_2)$, then $x_1 \in u_1 \mathbin{\text{Ш}} v_1$ and $x_2 \in u_2 \mathbin{\text{Ш}} v_2$. It follows that $x_1x_2 \in u_1u_2 \mathbin{\text{Ш}} u_2v_2$ and thus $(u_1u_2, v_1v_2) \in \sigma(x_1x_2)$. Conversely, if $(u, v) \in \sigma(x_1x_2)$, then $x_1x_2 \in u \mathbin{\text{Ш}} v$. Therefore, u and v can be decomposed as $u = u_1u_2$, $v = v_1v_2$ in such a way that $x_1 \in u_1 \mathbin{\text{Ш}} v_1$ and $x_2 \in u_2 \mathbin{\text{Ш}} v_2$. It follows that $(u, v) \in \sigma(x_1)\sigma(x_2)$. $\square$

Let $\mathcal{S}$ be a set of languages. A language K admits a *sequential decomposition* over $\mathcal{S}$ if $\tau(K)$ is a finite union of sets of the form $L \times R$, where $L, R \in \mathcal{S}$.

A language K admits a *parallel decomposition* over $\mathcal{S}$ if $\sigma(K)$ is a finite union of sets of the form $L \times R$, where $L, R \in \mathcal{S}$.

A *sequential (resp. parallel) system* is a finite set $\mathcal{S}$ of languages such that each member of $\mathcal{S}$ admits a sequential (resp. parallel) decomposition over $\mathcal{S}$. A language is *sequentially decomposable* if it belongs to some sequential system. It is *decomposable* if it belongs to a system which is both sequential and parallel. Thus, for each decomposable language L, one can find a sequential and parallel system $\mathcal{S}(L)$ containing L.

Theorem 3.2 *Let K be a language of A^*. The following conditions are equivalent:*

(1) *K is rational,*

(2) *$\tau(K)$ is recognizable,*

(3) *K is sequentially decomposable.*

Proof. (1) implies (3). Let K be a rational language and let $\mathcal{A}$ be the minimal automaton of K. For each state p, q of $\mathcal{A}$, let $K_{p,q}$ be the language accepted by $\mathcal{A}$ with p as initial state and q as unique final state. Let $\mathcal{S}$ be the set of finite unions of languages of the form $K_{p,q}$. Since $\mathcal{A}$ is finite, $\mathcal{S}$ is a finite set. We claim that

$$\tau(K_{p,q}) = \bigcup_{r \in Q} K_{p,r} \times K_{r,q} \tag{1}$$

Indeed, if, for some state r, $u \in K_{p,r}$ and $v \in K_{r,q}$, then $p{\cdot}u = r$ and $r{\cdot}v = q$ in $\mathcal{A}$. It follows that $uv \in K_{p,q}$ and $(u,v) \in \tau(K_{p,q})$. Conversely, let $(u,v) \in \tau(K_{p,q})$ and let $r = p{\cdot}u$. Since $uv \in K_{p,q}$, $p{\cdot}uv = q$, and thus $r{\cdot}v = q$, whence $v \in K_{r,q}$. Thus $(u,v) \in K_{p,r} \times K_{r,q}$.
It follows from (1) that each language of $\mathcal{S}$ admits a sequential decomposition on $\mathcal{S}$. Thus $\mathcal{S}$ is a sequential system and K itself is sequentially decomposable.

(3) implies (1) (Arnold, Carton). Let $\mathcal{S}$ be a sequential system containing K, and let $\sim_{\mathcal{S}}$ be the equivalence on A^* defined by $u \sim_{\mathcal{S}} v$ if, for every $F \in \mathcal{S}$, $u \in F$ is equivalent to $v \in F$. Clearly, $\sim_{\mathcal{S}}$ is an equivalence of finite index, which saturates K by definition. Therefore, it suffices to show that $\sim_{\mathcal{S}}$ is a congruence. Suppose that $u \sim_{\mathcal{S}} v$ and let F be a language of $\mathcal{S}$. Let $w \in A^*$ and suppose that $uw \in F$. Since F is sequentially decomposable over $\mathcal{S}$, there exist two languages $L, R \in \mathcal{S}$ such that $u \in L$, $w \in R$ and $LR \subset F$. It follows that $v \in L$, since $u \sim_{\mathcal{S}} v$, and thus $vw \in F$. Similarly, $vw \in F$ implies $uw \in F$ and thus $uw \sim_{\mathcal{S}} vw$. A dual argument would show that $wu \sim_{\mathcal{S}} wv$, which concludes the proof.

(2) implies (1). Suppose that $\tau(K)$ is recognizable. Observing that

$$\tau(K) \cap \{1\} \times A^* = \{1\} \times K$$

it follows by McKnight's theorem, that $\{1\} \times K$ is rational. Now $K = \pi(\{1\} \times K)$, where π denotes the second projection from $A^* \times A^*$ onto A^*. It follows by Proposition 2.3 that K is rational.

(3) implies (2). If K is sequentially decomposable, it belongs to some sequential system $\mathcal{S}$. By definition, each element of $\mathcal{S}$ is sequentially decomposable and thus is rational, since (3) implies (1). Furthermore, $\tau(K)$ is a finite union of languages of the form $L \times R$, where $L, R \in \mathcal{S}$. It follows, by Mezei's theorem, that $\tau(K)$ is recognizable. $\square$

It follows that every decomposable language is rational. Another important consequence is the following:

Proposition 3.3 *For each decomposable language K, $\sigma(K)$ is recognizable.*

Proof. Indeed, if $\mathcal{S}$ is a parallel and sequential system for K, every language of $\mathcal{S}$ is decomposable and hence rational, by Theorem 3.2. Since is sequentially decomposable over $\mathcal{S}$, $\sigma(K)$ is a finite union of languages of the form $L \times R$, where $L, R \in \mathcal{S}$. It follows, by Mezei's theorem, that $\sigma(K)$ is recognizable. □

We shall see later that the converse does not hold. That is, there exist a rational, indecomposable language K such that $\sigma(K)$ is recognizable. However, Proposition 3.3 remains a powerful tool for proving that a language is not decomposable. The most important example was already given in [5].

Proposition 3.4 (Schnoebelen) *The set $\sigma((ab)^*)$ is not recognizable. In particular, the language $(ab)^*$ is not decomposable.*

Proof. Let $K = (ab)^*$. Suppose that

$$\sigma(K) = \bigcup_{1 \leq i \leq n} L_i \times R_i$$

Then, for every $k \geq 0$, $(a^k, b^k) \in \sigma(K)$ since $(ab)^k \in a^k \text{Ш}\, b^k$. It follows that one of the blocks $L_i \times R_i$ contains two distinct pairs (a^r, b^r) and (a^s, b^s) with $r \neq s$. It follows that (a^r, b^s) also belongs to this block, and hence $a^r \text{Ш}\, b^s$ should contain a word of $(ab)^*$, a contradiction. □

4 Closure properties of decomposable languages

The following closure properties were established in [5], where the closure under shuffle is credited to Arnold. For the convenience of the reader, we give a self-contained proof.

Proposition 4.1 *Decomposable languages are closed under finite union, product and shuffle.*

Proof. Let K and K' be decomposable languages. Let $\mathcal{S}$ (resp. $\mathcal{S}'$) be a sequential and parallel system for K (resp. K'). Then $\mathcal{S} \cup \mathcal{S}' \cup \{K \cup K'\}$ is a sequential and parallel system for $K \cup K'$. Let us show that

$$\mathcal{R} = \mathcal{S} \cup \mathcal{S}' \cup \{XX' \mid X \in \mathcal{S} \text{ and } X' \in \mathcal{S}'\}$$

is a sequential and parallel system for KK'. Assume that

$$\sigma(K) = \bigcup_{1 \leq i \leq n} L_i \times R_i \quad \text{and} \quad \sigma(K') = \bigcup_{1 \leq j \leq n'} L'_j \times R'_j$$

Since σ is a substitution by Proposition 3.1,

$$\sigma(KK') = \bigcup_{\substack{1\le i\le n\\ 1\le j\le n'}} L_iL'_j \times R_iR'_j$$

Furthermore, if

$$\tau(K) = \bigcup_{1\le i\le n} L_i \times R_i \quad \text{and} \quad \tau(K') = \bigcup_{1\le j\le n'} L'_j \times R'_j$$

then

$$\tau(KK') = \bigcup_{1\le i\le n} (L_i \times R_iK') \cup \bigcup_{1\le j\le n} (KL'_i \times R'_i)$$

It follows that KK' is decomposable. Finally, the system

$$\mathcal{T} = \{X ш X' \mid X \in \mathcal{S} \text{ and } X' \in \mathcal{S}'\}$$

is a sequential and parallel system for $K ш K'$. Indeed, we have, with the previous notation,

$$\tau(K ш K') = \bigcup_{\substack{1\le i\le n\\ 1\le j\le n'}} (L_i ш L'_j) \times (R_i ш R'_j)$$
$$\sigma(K ш K') = \bigcup_{\substack{1\le i\le n\\ 1\le j\le n'}} (L_i ш R'_i) \times (L_j ш R'_j)$$

Therefore $K ш K'$ is decomposable. $\square$

We establish some new closure properties. We first consider inverse morphisms. We shall see later (Proposition 7.7) that decomposable languages are not closed under inverse morphisms. However, closure under inverse morphisms holds for a restricted class of morphisms. Recall that a morphism $\varphi : A^* \to B^*$ is *length preserving* (or *litteral*, or *strictly alphabetic*) if each letter of A is mapped onto a letter of B.

Lemma 4.2 *Let $\varphi : A^* \to B^*$ be a morphism and let K be a language of B^*. If*

$$\tau(K) = \bigcup_{1\le i\le n} L_i \times R_i$$

then

$$\tau(\varphi^{-1}(K)) = \bigcup_{1\le i\le n} \varphi^{-1}(L_i) \times \varphi^{-1}(R_i)$$

Furthermore, if φ is length preserving, and if

$$\sigma(K) = \bigcup_{1\le i\le n} L_i \times R_i$$

then

$$\sigma(\varphi^{-1}(K)) = \bigcup_{1\le i\le n} \varphi^{-1}(L_i) \times \varphi^{-1}(R_i)$$

Proof. The first result follows from the following sequence of equivalences

$$\begin{aligned}
(u,v) \in \tau(\varphi^{-1}(K)) &\iff uv \in \varphi^{-1}(K)\\
&\iff \varphi(uv) \in K\\
&\iff \varphi(u)\varphi(v) \in K\\
&\iff \text{ for some } i \in \{1,..,n\},\ (\varphi(u),\varphi(v)) \in L_i \times R_i\\
&\iff \text{ for some } i \in \{1,..,n\},\ (u,v) \in \varphi^{-1}(L_i) \times \varphi^{-1}(R_i)
\end{aligned}$$

If φ is length preserving, then a word w belongs to u Ш v if and only if $\varphi(w)$ belongs to $\varphi(u)$ Ш $\varphi(v)$. Therefore, the following sequence of equivalences holds:

$$\begin{aligned}
(u,v) \in \sigma(\varphi^{-1}(K)) &\iff (u \text{ Ш } v) \cap \varphi^{-1}(K) \neq \emptyset\\
&\iff (\varphi(u) \text{ Ш } \varphi(v)) \cap K \neq \emptyset\\
&\iff (\varphi(u),\varphi(v)) \in \sigma(K)\\
&\iff \text{ for some } i \in \{1,..,n\},\ (\varphi(u),\varphi(v)) \in L_i \times R_i\\
&\iff \text{ for some } i \in \{1,..,n\},\ (u,v) \in \varphi^{-1}(L_i) \times \varphi^{-1}(R_i)
\end{aligned}$$

This proves the second part of the lemma. □

Proposition 4.3 *Decomposable languages are closed under inverse of length preserving morphisms.*

Proof. Let $\varphi : A^* \to B^*$ be a length preserving (or letter to letter) morphism. Let K be a decomposable language of B^* and let $\mathcal{S}$ be a sequential and parallel system for K. By Lemma 4.2, the set $\{\varphi^{-1}(L) \mid L \in \mathcal{S}\}$ is a sequential and parallel system for $\varphi^{-1}(K)$. □

Proposition 4.4 *Decomposable languages are closed under left and right quotients.*

Proof. Let $\mathcal{S}$ be a sequential and parallel system for L and let $a \in A$. Let

$$\tau(L) = \bigcup_{1 \le i \le n} L_i \times R_i$$

Observing that $\{a\} \times a^{-1}L \subseteq \tau(L)$, we set

$$J = \{j \mid a \in L_j \text{ and } a^{-1}L \cap R_j \neq \emptyset\}$$

We claim that $a^{-1}L = \bigcup_{j \in J} R_j$. Indeed, if $u \in a^{-1}L$, then $au \in L$ and $(a,u) \in \tau(L)$. Therefore, $(a,u) \in L_j \times R_j$ for some j. But since $a \in L_j$ and $u \in a^{-1}L \cap R_j$, j belongs to J. Thus $u \in \bigcup_{j \in J} R_j$. Conversely, if $u \in R_j$ for some $j \in J$, then $a \in L_j$ and hence $(a,u) \in \tau(L)$, whence $au \in L$ and $u \in a^{-1}L$.

It follows from the claim that $a^{-1}L$ is a finite union of elements of $\mathcal{S}$. Since the elements of $\mathcal{S}$ are decomposable, $a^{-1}L$ is decomposable.

A symmetrical argument would show that La^{-1} is decomposable. □

The next result was proved by in [5].

Proposition 4.5 (Schnoebelen) *Every commutative rational language is decomposable.*

Proof. Let L be a commutative rational language. We claim that $\tau(L) = \sigma(L)$. Indeed, if $uv \in L$, then $u \text{ ш } v \cap L \neq \emptyset$. Conversely, if $u \text{ ш } v$ meets L, there exist two facorizations $u = u_0u_1 \cdots u_k$ and $v = v_1v_2 \cdots v_k$ such that $u_0v_1u_1 \cdots v_ku_k \in L$. It follows, since L is commutative, that $uv \in L$. It follows from the claim that any sequential decomposition of L is also a parallel decomposition. Now, by Theorem 3.2, L has a sequential decomposition. Therefore, L is decomposable. □

Since, by Proposition 4.1, decomposable languages are closed under union and product. Denote by Pol($\mathcal{C}om$) the *polynomial closure* of commutative languages, that is, the finite union of products of commutative languages. This class of languages includes the finite and the cofinite languages and the languages of concatenation level 3/2.

Theorem 4.6 (Schnoebelen) *Every language of Pol($\mathcal{C}om$) is decomposable.*

Schnoebelen has conjectured that a language is decomposable if and only if it belongs to Pol($\mathcal{C}om$). We shall disprove this conjecture in several ways and offer an improved conjecture. First, we remind the reader of a result of [4].

Theorem 4.7 (Pin-Weil) *A recognizable language gelongs to Pol($\mathcal{C}om$) if and only if its syntactic ordered monoid belongs to the positive variety* $[\![x^\omega y x^\omega \leq x^\omega]\!] \circledM \mathbf{Com}$.

We shall see later that decomposable languages are not closed under intersection. However, Arnold has shown they are closed under intersection with a commutative recognizable language. This result is based on the following property.

Proposition 4.8 *Let K and L be languages. Then $\tau(K \cap L) = \tau(K) \cap \tau(L)$. Furthermore, if one of the languages is commutative, $\sigma(K \cap L) = \sigma(K) \cap \sigma(L)$.*

Proof. The first formula follows from the following sequence of equivalent statements:

$$\begin{aligned}(u, v) \in \tau(K \cap L) &\iff uv \in K \cap L \iff uv \in K \text{ and } uv \in L \\ &\iff (u, v) \in \tau(L) \text{ and } (u, v) \in \tau(K)\end{aligned}$$

The inclusion $\sigma(K \cap L) \subseteq \sigma(K) \cap \sigma(L)$ is trivial. Assume that L is commutative and let $(u, v) \in \sigma(K) \cap \sigma(L)$. Since L is commutative, $\sigma(L) = \tau(L)$ and hence $uv \in L$. Furthermore there exist a word w of K such that $w = u_0v_1u_1 \cdots v_nu_n$ for some factorizations $u = u_0u_1 \cdots u_n$ and $v = v_1v_2 \cdots v_n$ of u and v. Now uv and w are commutatively equivalent, and thus $w \in K \cap L$. It follows that (u, v) belongs to $\sigma(K \cap L)$ and hence $\sigma(K \cap L) = \sigma(K) \cap \sigma(L)$. □

Corollary 4.9 (Arnold) *The intersection of a decomposable language with a commutative recognizable language is decomposable*

Proof. □

Proposition 4.8 can also be used to give a non-trivial examples of indecomposable language.

Proposition 4.10 *Let $A = \{a, b, c\}$. The language $(ab)^*cA^*$ is not decomposable.*

Proof. Let $L = (ab)^*cA^*$. If L is decomposable, the language

$$Lc^{-1} = (ab)^* \cup (ab)^*cA^*$$

is decomposable by Proposition **??**. The intersection of this language with the recognizable commutative language $\{a, b\}^*$ is equal to $(ab)^*$, and thus by Corollary 4.9 $(ab)^*$ should also be decomposable. But this contradicts Proposition 3.4 and thus L is not decomposable. □

5 Schnoebelen's conjecture

In this section, we disprove Schoebelen's conjecture by giving an example of a decomposable language which is not a finite union of products of commutative languages.

Let u and v be two words of A. A word $u = a_1a_2 \cdots a_k$ is said to be a *subword* of v if v can be factorized as $v = v_0a_1v_1 \cdots a_kv_k$ where $v_0, v_1, \ldots, v_k \in A^*$. Following Eilenberg [2], we set

$$\binom{v}{u} = \mathrm{Card}\{(v_0, v_1, \ldots, v_k) \in A^* \times A^* \times \cdots \times A^* \mid v_0a_1v_1 \cdots a_kv_k = v\}$$

Thus $\binom{v}{u}$ is the number of distinct ways to write u as a subword of v. For instance, $\binom{aabbaa}{aba} = 8$ and $\binom{a^n}{a^m} = \binom{n}{m}$. The basic properties of these *binomial coefficients* are summarized by the following formulae

(1) For every word $u \in A^*$, $\binom{u}{1} = 1$.

(2) For every non-empty word $u \in A^*$, $\binom{1}{u} = 0$.

(3) If $w = uv$, then $\binom{w}{x} = \sum_{x_1x_2=x} \binom{u}{x_1}\binom{v}{x_2}$.

Let $A = \{a, b\}$ be an alphabet, and let K be the language of words x over the alphabet A such that $\binom{x}{ab} \equiv 1 \mod 2$. The minimal automaton of this language is represented in Figure 5.1.

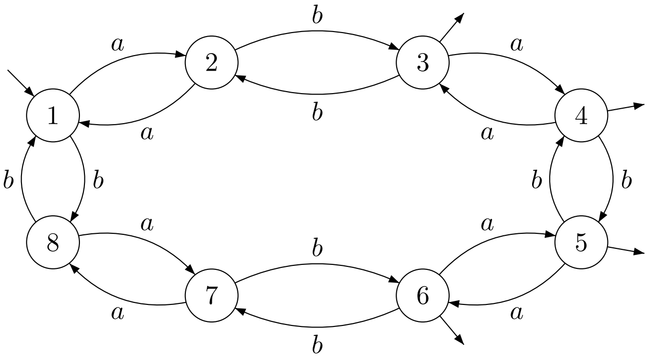


Figure 5.1: An automaton for M.

The syntactic monoid of K is a non-abelian group with eight elements.
For $i, j, k \in \{0,1\}$ and $c \in A$, let us set

$$M_k^{i,j} = \Big\{x \in A^* \mid |x|_a \equiv i \bmod 2,\ |x|_b \equiv j \bmod 2 \text{ and } \binom{x}{ab} \equiv k \bmod 2\Big\}$$
$$M^{i,j} = \Big\{x \in A^* \mid |x|_a \equiv i \bmod 2,\ |x|_b \equiv j \bmod 2\Big\}$$
$$M_c^{i,j} = M^{i,j} \cap A^*cA^*$$

Let $\mathcal{F}$ be the set of languages that are finite union of languages of the form $M_k^{i,j}$, $M_c^{i,j}$ or $\{1\}$. Observe that, since

$$M^{i,j} = M_0^{i,j} \cup M_1^{i,j}$$

$M^{i,j}$ belongs to $\mathcal{F}$. We claim that $\mathcal{F}$ is a sequential and parallel system. We first show it is a sequential system by proving that the languages $M_k^{i,j}$, $M_c^{i,j}$ or $\{1\}$ have a sequential decomposition over $\mathcal{F}$. This is the purpose of the next proposition.

Proposition 5.1
(a) $\tau(1) = \{1\} \times \{1\}$
(b) *For* $i, j, k \in \{0,1\}$,

$$\tau(M_h^{i,j}) = \bigcup_{\substack{k+m \equiv i \bmod 2 \\ \ell+n \equiv j \bmod 2 \\ h \equiv p+q+kn \bmod 2}} (M_p^{k,\ell} \times M_q^{m,n}) \tag{2}$$

(c) *For* $i, j \in \{0,1\}$, *and any* $c \in A$,

$$\tau(M_c^{i,j}) = \bigcup_{\substack{k+m \equiv i \bmod 2 \\ \ell+n \equiv j \bmod 2}} (M_c^{k,\ell} \times M^{m,n}) \bigcup_{\substack{k+m \equiv i \bmod 2 \\ \ell+n \equiv j \bmod 2}} (M^{m,n} \times M_c^{k,\ell}) \tag{3}$$

Proof. (a) is trivial.
(b) Let $(u,v) \in \tau(M_h^{i,j})$, that is, $uv \in M_h^{i,j}$. Define $k, \ell, m, n, p, q \in \{0,1\}$ by the conditions $|u|_a \equiv k \bmod 2$, $|u|_b \equiv \ell \bmod 2$, $\binom{u}{ab} \equiv p \bmod 2$, $|v|_a \equiv m \bmod 2$, $|v|_b \equiv n \bmod 2$ and $\binom{v}{ab} \equiv q \bmod 2$. By definition, $u \in M_p^{k,\ell}$ and $v \in M_q^{m,n}$.

Furthermore, since $|uv|_a \equiv i \bmod 2$ and $|uv|_b \equiv j \bmod 2$, $k + m \equiv i \bmod 2$ and $\ell + n \equiv j \bmod 2$. Finally, since $\binom{u}{ab} \equiv h \bmod 2$, the formula

$$\binom{uv}{ab} \equiv \binom{u}{ab} + \binom{v}{ab} + |u|_a|v|_b \equiv p + q + kn \mod 2 \tag{4}$$

shows that $p + q + kn \equiv h \bmod 2$. This proves that (u, v) belongs to the right hand side of (2).

In the opposite direction, let $u \in M_p^{k,\ell}$ and $v \in M_q^{m,n}$, with $k+m \equiv i \bmod 2$, $\ell + n \equiv j \bmod 2$ and $h \equiv p + q + kn \bmod 2$. Then $|uv|_a \equiv k + m \equiv i \bmod 2$, $|uv|_b \equiv \ell + n \equiv j \bmod 2$, and, by Formula (4), $\binom{u}{ab} \equiv p + q + kn \equiv h \bmod 2$.

(c) Let $(u, v) \in \tau(M_c^{i,j})$, that is, $uv \in M_c^{i,j}$. Define $k, \ell, m, n \in \{0, 1\}$ by the conditions $|u|_a \equiv k \bmod 2$, $|u|_b \equiv \ell \bmod 2$, $|v|_a \equiv m \bmod 2$ and $|v|_b \equiv n \bmod 2$. Since $|uv|_a \equiv i \bmod 2$ and $|uv|_b \equiv j \bmod 2$, the relations $k + m \equiv i \bmod 2$ and $\ell + n \equiv j \bmod 2$ hold. Furthermore, since $uv \in M_c^{i,j}$, the letter c occurs at least once in uv. Thus it occurs in u or in v and hence $(u, v) \in (M_c^{k,\ell} \times M^{m,n}) \cup (M^{m,n} \times M_c^{k,\ell})$.

In the opposite direction, let $u \in M_c^{k,\ell}$ and $v \in M^{m,n}$, with $k+m \equiv i \bmod 2$ and $\ell + n \equiv j \bmod 2$ (the proof would be similar for $u \in M^{k,\ell}$ and $v \in M_c^{m,n}$). Then $|uv|_a \equiv k + m \equiv i \bmod 2$, $|uv|_b \equiv \ell + n \equiv j \bmod 2$, and since $|u|_c > 0$, $|uv|_c > 0$ and $uv \in M_c^{i,j}$, that is, $(u, v) \in \tau(M_c^{i,j})$. □

We now prove that $\mathcal{F}$ is a parallel system. The proof relies on a simple, but useful observation.

Lemma 5.2 *For any words $x, y \in A^*$, $\binom{xaby}{ab} = \binom{xbay}{ab} + 1$.*

Proof. We have on the one hand

$$\binom{xaby}{ab} = \binom{y}{ab} + \binom{xa}{a}\binom{by}{b} + \binom{x}{ab} = \binom{y}{ab} + (|x|_a + 1)(|y|_b + 1) + \binom{x}{ab}$$

and, on the other hand

$$\binom{xbay}{ab} = \binom{ay}{ab} + \binom{xb}{a}\binom{ay}{b} + \binom{xb}{ab} = \binom{y}{ab} + |y|_b + |x|_a|y|_b + |x|_a + \binom{x}{ab}$$

which proves the lemma. □

Proposition 5.3

(a) $\sigma(1) = \{1\} \times \{1\}$

(b) *For any $i, j \in \{0, 1\}$,*

$$\sigma(M_0^{i,j}) = \bigcup_{\substack{k+m\equiv i \bmod 2 \\ \ell+n\equiv j \bmod 2}} (M^{k,\ell} \times M^{m,n}) \tag{5}$$

(c) *For any $i, j \in \{0, 1\}$,*

$$\sigma(M_1^{i,j}) = \bigcup_{\substack{k+m\equiv i \bmod 2 \\ \ell+n\equiv j \bmod 2}} \Big((M_a^{k,\ell} \times M_b^{m,n}) \cup (M_b^{k,\ell} \times M_a^{m,n})\Big) \cup (\{1\} \times M_1^{i,j}) \cup (M_1^{i,j} \times \{1\}) \tag{6}$$

(d) *For any $i, j \in \{0,1\}$, for any $c \in A$, $\sigma(M_c^{i,j}) = \tau(M_c^{i,j})$.*

Proof. (a) is trivial.
(b) Let $(u,v) \in \sigma(M_0^{i,j})$, and let $w \in (u \text{ Ш } v) \cap M^{i,j}$. Define $k, \ell, m, n \in \{0,1\}$ by the conditions $|u|_a \equiv k \bmod 2$, $|u|_b \equiv \ell \bmod 2$, $|v|_a \equiv m \bmod 2$ and $|v|_b \equiv n \bmod 2$. Then $(u,v) \in M^{k,\ell} \times M^{m,n}$. Furthermore, since $|w|_a \equiv i \bmod 2$ and $|w|_b \equiv j \bmod 2$, the relations $k + m \equiv i \bmod 2$ and $\ell + n \equiv j \bmod 2$ hold. Thus (u,v) belongs to the right hand side of (5).

Conversely, let $(u,v) \in M^{k,\ell} \times M^{m,n}$ with $k + m \equiv i \bmod 2$ and $\ell + n \equiv j \bmod 2$. First, if $(u,v) \in (A^*aA^* \times A^*bA^*) \cup (A^*bA^* \times A^*aA^*)$, then $\{u,v\} = \{(x_1ay_1, x_2by_2)\}$ for some words $x_1, x_2, y_1, y_2 \in A^*$. Setting $x = x_1x_2$ and $y = y_1y_2$, the set $u \text{ Ш } v$ contains the words $xaby$ and $xbay$. Note that $|xaby|_a = |xbay|_a = |uv|_a \equiv i \mod 2$ and $|xaby|_b = |xbay|_b = |uv|_b \equiv i \mod 2$. It follows by Lemma 5.2 that one of these words is in $M_0^{i,j}$ and thus $(u,v) \in \sigma(M_0^{i,j})$. If now, $(u,v) \notin (A^*aA^* \times A^*bA^*) \cup (A^*bA^* \times A^*aA^*)$, then $(u,v) \in (a^* \times a^*) \cup (b^* \times b^*)$ and thus $\binom{uv}{ab} = 0$. Therefore $uv \in M_0^{i,j}$ and $(u,v) \in \sigma(M_0^{i,j})$.
(c) The proof of is quite similar to that of (b). Let $(u,v) \in \sigma(M_1^{i,j})$, and let $w \in (u \text{ Ш } v) \cap M^{i,j}$. Since $\binom{w}{ab} \equiv 1 \bmod 2$, $|w|_a > 0$ and $|w|_b > 0$.
(d) holds, since $M_c^{i,j}$ is a commutative language. □

Theorem 5.4 *The language K is decomposable.*

Proof. Indeed, K belongs to the parallel and sequential system $\mathcal{F}$, since $K = \bigcup_{0 \le i,j \le 1} M_1^{i,j}$. □

It remains to show that K does not belong to $\mathrm{Pol}(\mathcal{C}om)$. By Theorem 4.7, the syntactic monoid of a language of $\mathrm{Pol}(\mathcal{C}om)$ belongs to the variety $[\![x^\omega y x^\omega \le x^\omega]\!] \circledM \mathbf{Com}$. But this variety is contained in $\mathbf{A} \circledM \mathbf{Com}$ and, by a well-known result, every group in this variety is commutative. Since the syntactic monoid of K is a non-commutative group, K is not in $\mathrm{Pol}(\mathcal{C}om)$.

6 Non decomposable languages

In this section, we give several examples of non decomposable languages. We first generalize Proposition 3.4 to a larger class of languages.

Proposition 6.1 *Let u and v be two words of A^* such that $uv \neq vu$. Then $\sigma((uv)^*)$ is not recognizable. In particular, the language $(uv)^*$ is not recognizable.*

Proof. We first remind the reader with a classical result of combinatorics on words (see [3]): two words commute if and only if they are powers of the same word. Next we claim that $\sigma((uv)^*)$ is recognizable if and only if $\sigma((vu)^*)$ is recognizable. Indeed, $(vu)^* = \{1\} \cup v(uv)^*u$ and since σ is a substitution,

$$\sigma((vu)^*) = \sigma(1) \cup \sigma(v)\sigma((uv)^*)\sigma(u)$$

Now $\sigma(1)$, $\sigma(u)$ and $\sigma(v)$ are finite and, by Mezei's theorem, belong to $\mathrm{Rec}(A^* \times A^*)$. Furthermore, $\mathrm{Rec}(A^* \times A^*)$ is closed under union and product. It follows that if $\sigma((uv)^*)$ is recognizable, so is $\sigma((vu)^*)$. The converse also holds by duality, which proves the claim.

We can now assume, without loss of generality, that $|u| \leq |v|$. Let $K = (uv)^*$. If $\sigma(K)$ is recognizable, it can be written as a finite union of blocks $L \times R$, where $L, R \in \mathrm{Rec}(A^*)$. For each $n \geq 0$, $(uv)^n \in u^n ш v^n$, and hence $(u^n, v^n) \in \sigma(K)$. Therefore, there exists a block $L \times R$ such that the set

$$S = \{n \in \mathbb{N} \mid (u^n, v^n) \in L \times R\}$$

is infinite. Let $s = \min S$. By assumption, we have $u^s \in L$ and $v^n \in R$ for each $n \in S$ and thus $(u^s ш v^n) \cap (uv)^* \neq \emptyset$.

Let us fix $n \geq 4s|u|$ and let k be such that $(uv)^k \in u^s ш v^n$. There exist two factorizations $u^s = x_0 \cdots x_{\ell+1}$ and $v^n = y_1 \cdots y_\ell$ such that $x_0, x_{\ell+1} \in A^*$, $x_1, y_1, \ldots, x_\ell, y_\ell \in A^+$ and $x_0 y_1 x_1 \cdots x_\ell y_\ell x_{\ell+1} = (uv)^k$. It follows, by the choice of n

$$|y_1 \cdots y_\ell| = n|v| \geq 4s|u||v|$$

Now, since $\ell \leq |x_1 \cdots x_\ell| \leq s|u|$, one of the words y_i has length $\geq 4|v|$. Now, since y_i is a factor of $(uv)^k$ and since $|u| \leq |v|$, y_i contains vuv as a factor. At the same time, y_i is a factor of v^n of length $\geq 4|v|$, that is, a factor of v^5. It follows that vuv is a factor of v^5. Let us write v as the power of some primitive word, say $v = t^p$. Then tut is a factor of vuv, which is in turn a factor of t^{5p}. Now, a primitive word cannot have any conjugate, which means that if $t^{5p} = xtuty$, then x and y are necessarily powers of t. But this forces u itself to be a power of t, a contradiction, since u and v are not powers of the same word. Thus $\sigma(K)$ is not recognizable. $\square$

7 Inverse morphisms

In this section, we show that decomposable languages are not closed under inverse morphisms.

Let L be the language defined over the alphabet $A = \{a, b\}$ by the following regular expression:

$$L = (aab)^* \cup A^* b (aa)^* ab A^*$$

We claim that this language is decomposable. The minimal automaton of L is represented in Figure 7.2.

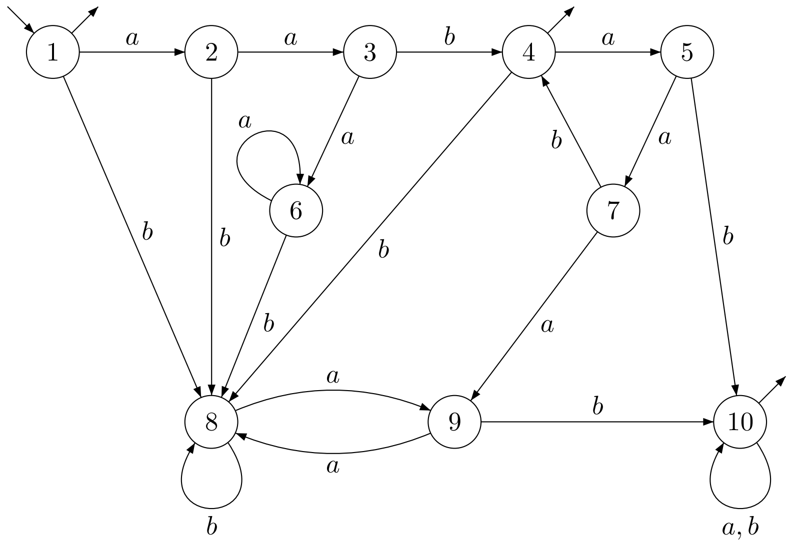


Figure 7.2: The minimal automaton of L.

Its ordered syntactic monoid $(M, \leq)$ is presented by the relations $bbb = bb$, $aaab = abb$, $aabb = bb$, $abab = 0$, $baaa = bba$, $baab = b$, $bab = 0$, $bbaa = bb$, $bbab = 0$ and $aaaaa = aaa$. Thus M contains the elements

$$\{1, a, b, a^2, ab, ba, b^2, a^3, a^2b, aba, ab^2, ba^2, bab, b^2a, a^4, a^2ba, aba^2, ab^2a, a^2ba\}$$

The order relation is defined by $0 \leq x$ for all $x \in M$ and $1 < a^4$, $a < a^3$, $a^2ba < a$, $aba^2 < a$, $b < bb$, $a^2 < a^4$, $abba < a^2$, $a^2ba^2 < a^2$, $ab < abb$, $ba < bba$, $a^2b < bb$, $ba^2 < bb$, $bb < a^4$, $a^2ba^2 < bb$, $abb < a^3$, $bba < a^3$, $aba < abba$, $aba^2 < abb$, $ba^2 < a^4$ and $a^2ba < bba$.

The $\mathcal{J}$-class structure of M is shown in Figure 7.3.

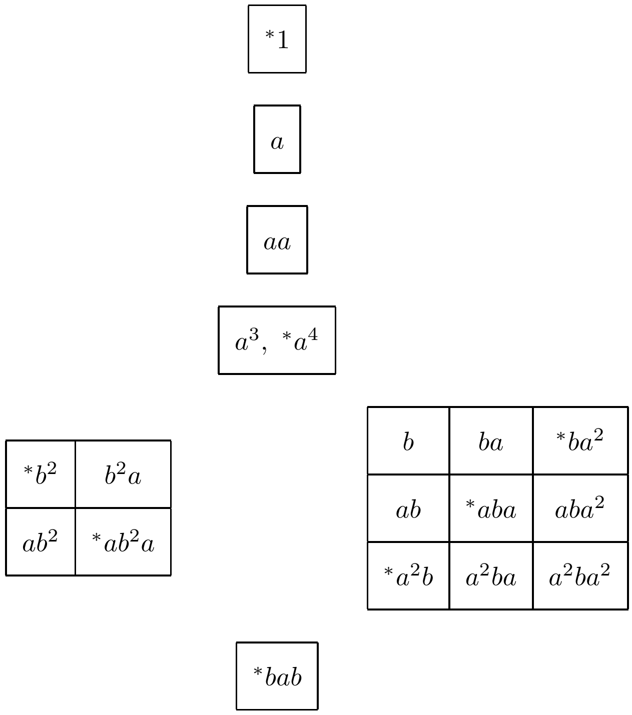


Figure 7.3: The $\mathcal{J}$-class structure of M.

The order relation of $(M, \leq)$ is shown in Figure 7.4.

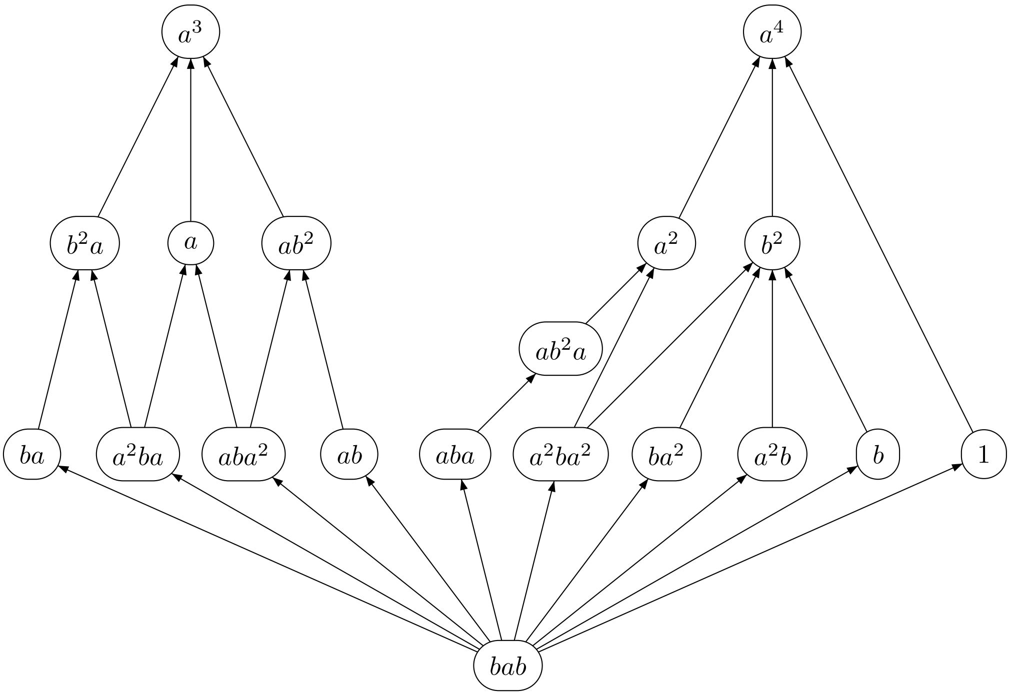


Figure 7.4: The order of M.

We now show that L is decomposable by constructing, step by step, a parallel and sequential system containing L. First, consider the automaton $\mathcal{A}$ represented in Figure 7.5.

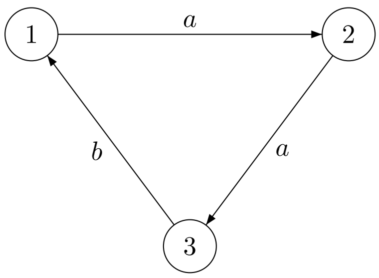


Figure 7.5: The automaton $\mathcal{A}$.

Let $K_{i,j}$ be the language accepted by $\mathcal{A}$ with i as initial state and j as the only final state. These languages are $K_{1,1} = (aab)^*$, $K_{1,2} = (aab)^*a$, $K_{1,3} = (aab)^*aa$, $K_{2,1} = (aba)^*ab$, $K_{2,2} = (aba)^*$, $K_{2,3} = (aba)^*a$, $K_{3,1} = (baa)^*b$, $K_{3,2} = (baa)^*ba$ and $K_{3,3} = (baa)^*$. In the next proposition, we compute the image by τ of these languages.

Proposition 7.1 *For* $1 \le i, j \le 3$,

$$\tau(K_{i,j}) = \bigcup_{1 \le k \le 3} (K_{i,k} \times K_{k,j})$$

Proof. If $(u, v) \in \tau(K_{i,j})$, then $uv \in K_{i,j}$, and thus $i \cdot uv = j$ in $\mathcal{A}$. Setting $k = i \cdot u$, we have $k \cdot v = j$ and thus $u \in K_{i,k}$ and $v \in K_{k,j}$. In the opposite direction, if $u \in K_{i,k}$ and $v \in K_{k,j}$, then $i \cdot u = k$ and $k \cdot v = j$, whence $i \cdot uv = j$ and $uv \in K_{i,j}$. $\square$

Let $L_0 = A^*b(aa)^*abA^*$. We first compute the image of L_0 under σ and τ.

Proposition 7.2

$$\tau(L_0) = (A^* \times L_0) \cup (L_0 \times A^*) \cup (A^*b(aa)^* \times a(aa)^*bA^*) \cup \\ (A^*b(aa)^*a \times (aa)^*bA^*)$$

Proof. Let $(u, v) \in \tau(L_0)$, that is, $uv \in L_0$. First suppose that $u \in L_0$ or $v \in L_0$, this implies that $(u, v) \in (A^* \times L_0)$ or $(u, v) \in (L_0 \times A^*)$. Otherwise we can write uv as $u_1b(aa)^nabv_1$ where $n \ge 0$, u_1 is a prefix of u and v_1 is a suffix of v, and then $(u, v) \in (A^*b(aa)^* \times a(aa)^*bA^*)$ or $(u, v) \in (A^*b(aa)^*a \times (aa)^*bA^*)$. In the opposite direction, if $u \in L_0$ its clear that for any $v \in A^*$, $uv, vu \in L_0$. Now suppose that $u = u_1b(aa)^n$ and $v = a(aa)^mbv_1$ (resp. $u = u_1(aa)^na$ and $v = (aa)^mbv_1$) for some $n, m \ge 0$, then $uv \in L_0$. $\square$

Proposition 7.3

$$\begin{aligned}\sigma(L_0) = \ & (L_0 \times A^*) \cup (A^* \times L_0) \cup (A^*aA^*bA^* \times A^*bA^*) \\ & \cup (A^*bA^*aA^* \times A^*bA^*) \cup (A^*bA^*bA^* \times A^*aA^*) \\ & \cup (A^*bA^* \times A^*aA^*bA^*) \cup (A^*bA^* \times A^*bA^*aA^*) \\ & \cup (A^*aA^* \times A^*bA^*bA^*)\end{aligned}$$

Proof. If $(u, v) \in \sigma(L_0)$, then by definition $(u \text{ Ш } v) \cap L_0 \neq \emptyset$. Let us take some $w \in (u \text{ Ш } v) \cap L_0$. By definition of L_0, w can be decomposed as $w = w_1w_2w_3$, where $w_1, w_3 \in A^*$ and $w_2 = ba^nb$ with n odd. Since $w \in u \text{ Ш } v$, w_2 can be written as $w_2 = u_1v_1 \cdots u_nv_n$ with $u_i, v_i \in A^*$ for $1 \le i \le n$, $u = u_0u_1 \cdots u_nu_{n+1}$ and $v = v_0v_1 \cdots v_nv_{n+1}$ for some $u_0, v_0, \ldots, u_{n+1}, v_{n+1} \in A^*$. Let us consider the words $\overline{u} = u_1 \cdots u_n$ and $\overline{v} = v_1 \cdots v_n$. Since $w_2 = ba^nb$, the words $\overline{u}$ and $\overline{v}$ can take the following values, where $n = n_1 + n_2$:

(1) $\overline{u} = ba^{n_1}b$ and $\overline{v} = a^{n_2}$

(2) $\overline{u} = a^{n_1}$ and $\overline{v} = ba^{n_2}b$

(3) $\overline{u} = ba^{n_1}$ and $\overline{v} = a^{n_2}b$

(4) $\overline{u} = a^{n_1}b$ and $\overline{v} = ba^{n_2}$

Let R be the right hand side of the equality to be proved. We show that $\sigma(L_0)$ is a subset of R by considering the four cases separately.
Case (1). If n_1 is odd, then $u \in L_0$, and so $(u, v) \in (L_0 \times A^*)$, otherwise, if n_1 is even, and $n_1 + n_2$ is odd, we have $n_2 > 0$, and then $(u, v) \in A^*bA^*bA^* \times A^*aA^*$.

Case (2). A proof similiar to that of case (1) shows that (u,v) belongs either to $A^* \times L_0$ or to $A^*aA^* \times A^*bA^*bA^*$.
Case (3). If $n_1 > 0$, $(u,v) \in A^*bA^*aA^* \times A^*bA^*$. Otherwise, since $n_1 + n_2$ is odd, $n_2 > 0$ and then $(u,v) \in A^*bA^* \times A^*aA^*bA^*$.
Case (4). A proof similiar to that of case (3) shows that (u,v) belongs either to $A^*bA^* \times A^*bA^*aA^*$ or to $A^*aA^*bA^* \times A^*bA^*$.

We now prove that R is a subset of $\sigma(L_0)$. If $(u,v) \in (L_0 \times A^*) \cup (A^* \times L_0)$, it is clear that $(u \text{ Ш } v) \cap L_0 \neq \emptyset$. Suppose that $(u,v) \in (A^*aA^*bA^* \times A^*bA^*)$. Observing that $A^*aA^*bA^* = A^*abA^*$, the word u can be decomposed as $u = u_1abu_2$ with $u_1, u_2 \in A^*$, and v can be decomposed as $v = v_1bv_2$ with $v_1, v_2 \in A^*$. Now $v_1u_1babv_2 \in (u \text{ Ш } v) \cap L_0$ and thus $(u,v) \in \sigma(L_0)$. The proof is similar if (u,v) belongs to $A^*bA^*aA^* \times A^*bA^*$, $A^*bA^* \times A^*bA^*aA^*$ or $A^*bA^* \times A^*aA^*bA^*$.

Finally, if $(u,v) \in A^*bA^*bA^* \times A^*aA^*$, then u can be decomposed as $u = u_1ba^nbu_2$ with $n \geq 0$, $u_1, u_2 \in A^*$, and v can be decomposed as $v = v_1av_2$ with $v_1, v_2 \in A^*$. If n is even, u and v can be shuffled as $u_1v_1ba^{(n+1)}bv_2u_2$, a word of L_0, otherwise, u and v can be shuffled as $u_1v_1ba^nbav_2u_2$, another word of L_0. Thus $(u,v) \in \sigma(L_0)$ in both cases. The proof for $A^*aA^* \times A^*bA^*bA^*$ is similar. □

For $1 \leq i,j \leq 3$, define the languages $L_{i,j}$ as the union of L_0 with the language $K_{i,j}$. We first compute the image of these languages under τ.

Proposition 7.4 *For $1 \leq i,j \leq 3$,*

$$\tau(L_{i,j}) = \tau(L_0) \cup \bigcup_{1 \leq k \leq 3} (L_{i,k} \times L_{k,j})$$

Proof. Let R be the right handside of the relation to be proved. Since $L_{i,j} = L_0 \cup K_{i,j}$, $\tau(L_{i,j}) = \tau(L_0) \cup \tau(K_{i,j})$. Now, by Proposition 7.1, $\tau(K_{i,j}) = \bigcup_{1 \leq k \leq 3}(K_{i,k} \times K_{k,j})$, and since each $K_{i,j}$ is a subset of $L_{i,j}$, $\tau(K_{i,j})$ is a subset of R. It follows that $\tau(L_{i,j})$ is a subset of R.

We now prove the opposite inclusion. Since L_0 is a subset of $L_{i,j}$, $\tau(L_0)$ is a subset of $\tau(L_{i,j})$. Furthermore, if $(u,v) \in L_{i,k} \times L_{k,j}$ for some k, two possibilities arise. First, if $u \in L_0$ or $v \in L_0$ then $(u,v) \in \tau(L_0)$ and hence $(u,v) \in \tau(L_{i,j})$. Otherwise, $u \in K_{i,k}$, $v \in K_{k,j}$, $uv \in K_{i,j}$ and thus $(u,v) \in \tau(L_{i,j})$. □

In order to compute the image of the languages $L_{i,j}$ under σ, we introduce the languages

$$M_{i,j} = K_{i,j} \cap a^*(b \cup 1)a^*$$

These languages are clearly finite and thus decomposable, and they belong to some parallel and sequential systems $\mathcal{S}(M_{i,j})$.

Proposition 7.5 *For $1 \leq i,j \leq 3$,*

$$\sigma(L_{i,j}) = \sigma(L_0) \cup \sigma(M_{i,j}) \cup (L_{i,j} \times \{1\}) \cup (\{1\} \times L_{i,j})$$

Proof. If $(u,v) \in \sigma(L_{i,j})$, then $(u \text{ Ш } v) \cap L_{i,j} \neq \emptyset$. First, if $u = 1$ or $v = 1$ then $(u,v) \in (L_{i,j} \times \{1\}) \cup (\{1\} \times L_{i,j})$. Now, suppose that u and v are non-empty words.

If $|u|_b + |v|_b < 2$ then necessarily $(u, v) \in \sigma(M_{i,j})$. Suppose that $|u|_b + |b|_v \geq 2$. We claim that $(u, v) \in (A^*aA^*bA^* \times A^*bA^*) \cup (A^*bA^*aA^* \times A^*bA^*) \cup (A^*bA^*bA^* \times A^*aA^*) \cup (A^*bA^* \times A^*aA^*bA^*) \cup (A^*bA^* \times A^*bA^*aA^*) \cup (A^*aA^* \times A^*bA^*bA^*) \subseteq \sigma(L_0)$. Since u and v are both non-empty, they contain at least one letter. If u and v are equal to b, $(u \text{ Ш } v) \cap L_0 = \emptyset$, and so u or v contains the letter a and since $|u|_b + |v|_b < 2$ the result holds. Conversely, if $(u, v) \in \sigma(L_0) \cup \sigma(M_{i,j}) \cup (L_{i,j} \times \{1\}) \cup (\{1\} \times L_{i,j})$ by the definition of $M_{i,j}$, Proposition 7.3 and the definition of $L_{i,j}$, $(u, v) \in \sigma(L_{i,j})$. □

We are now ready to show that L is decomposable. By Theorem 4.6, all languages which are products of commutative languages are decomposable. In particular, the following languages are decomposable: $A^*b(aa)^*$, $(aa)^*abA^*$, $A^*b(aa)^*a$ and $(aa)^*bA^*$, $A^*aA^*bA^*$, $A^*bA^*aA^*$, $A^*bA^*bA^*$, A^*aA^* and A^*bA^*.

Theorem 7.6 *The language L is decomposable.*

Proof. Let us define a system $\mathcal{S}$ consisting of the unions of the following languages: L_0, $\{1\}$, A^*, $L_{i,j}$, for $1 \leq i, j \leq 3$ and the languages of the systems $\mathcal{S}(A^*b(aa)^*)$, $\mathcal{S}((aa)^*abA^*)$, $\mathcal{S}(A^*b(aa)^*a)$, $\mathcal{S}((aa)^*bA^*)$, $\mathcal{S}(A^*aA^*bA^*)$, $\mathcal{S}(A^*bA^*aA^*)$, $\mathcal{S}(A^*bA^*bA^*)$, $\mathcal{S}(A^*aA^*)$, $\mathcal{S}(A^*bA^*)$ and $\mathcal{S}(M_{i,j})$ for $1 \leq i, j \leq 3$. Note that L belongs to $\mathcal{S}$ since $L = L_{1,1}$.

It remains to show that for any language L' of $\mathcal{S}$, $\tau(L')$ and $\sigma(L')$ can be written as the union of languages $(M \times N)$ where M and N belong to $\mathcal{S}$. For L_0, the result follows from Propositions 7.2 and 7.3. For $L_{i,j}$, the result follows from Propositions 7.4 and 7.5. Clearly, $\tau(\{1\}) = \sigma(\{1\}) = (\{1\} \times \{1\})$ and $\sigma(A^*) = \tau(A^*) = (A^* \times A^*)$. For any language of the systems described above, its image under τ and σ can be obtained from the languages of these systems, because they are parallel and sequential systems. Finally, since for any language N_1, N_2, the formulas $\tau(N_1 \cup N_2) = \tau(N_1) \cup \tau(N_2)$ and $\sigma(N_1 \cup N_2) = \sigma(N_1) \cup \sigma(N_2)$ hold, the system $\mathcal{S}$ is a parallel and sequential system. □

Proposition 7.7 *Decomposable languages are not closed under inverse morphism.*

Proof. Let $A = \{a, b\}$ and let $\varphi : A^* \to A^*$ be the morphism of monoids defined by $\psi(a) = aa$ and $\psi(b) = b$. If $L = (aab)^* \cup A^*b(aa)^*abA^*$, then $\varphi^{-1}(L) = (ab)^*$. Now L is decomposable by Theorem 7.6 but, by Proposition 3.4, $\varphi^{-1}(L)$ is not. □

Corollary 7.8 *Decomposable languages do not form a positive variety of languages.*

8 Intersection

In this section, we show that decomposable languages are not closed under intersection.

Let L_1 and L_2 be languages defined over the alphabet $A = \{a, b\}$ by the following regular expressions:

$$L_1 = (ab)^+ \cup (ab)^* bA^*$$
$$L_2 = (ab)^+ \cup (ab)^* aaA^*$$

We claim that these two languages are decomposable. The minimal automata for L_1 and L_2 are represented in Figure 8.6.

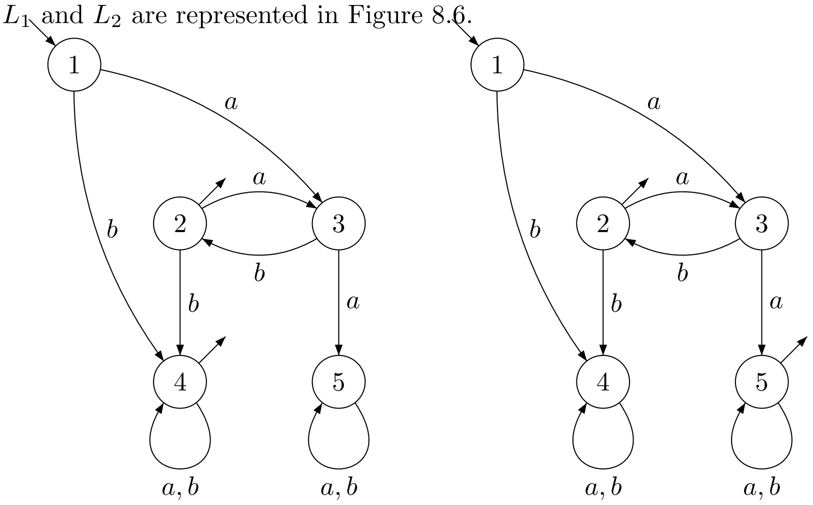


Figure 8.6: Automata for L_1 (on the left) and L_2 (on the right).

The languages L_1 and L_2 have the same syntactic monoid M but different syntactic order relations, denoted respectively by $\leq_{L_1}$ and $\leq_{L_2}$. The monoid M is presented by the relations $aaa = aa$, $aab = aa$, $aba = a$, $baa = abb$, $bab = b$, $bba = bb$ and $bbb = bb$. Thus M contains the elements

$$\{1, a, b, ab, ba, aa, baa, bb\}$$

The $\mathcal{J}$-class structure of M is shown in Figure 8.7.

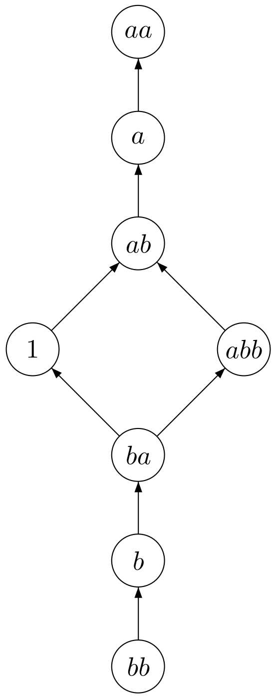
^{*1}

$^*ab$	a
b	$^*ba$

$^*aa$
$^*baa$
$^*bb$

Figure 8.7: The $\mathcal{J}$-class structure of M.

The order relation $\leq_{L_1}$ is defined by $bb \leq_{L_1} b$, $b \leq_{L_1} ba$, $ba \leq_{L_1} 1$, $ba \leq_{L_1} abb$, $1 \leq_{L_1} ab$, $abb \leq_{L_1} ab$, $ab \leq_{L_1} a$ and $a \leq_{L_1} aa$. The order relation $\leq_{L_2}$ is defined by $aa \leq_{L_2} ab$, $aa \leq_{L_2} a$, $ab \leq_{L_2} 1$, $ab \leq_{L_2} abb$, $a \leq_{L_2} abb$, $1 \leq_{L_2} ba$, $abb \leq_{L_2} ba$, $abb \leq_{L_2} b$, $ba \leq_{L_2} bb$ and $b \leq_{L_2} bb$. Both relations, $\leq_{L_1}$ and $\leq_{L_2}$, are represented in Figure 8.8.



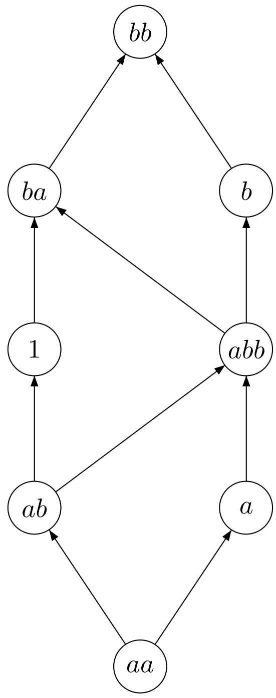


Figure 8.8: Order relations for L_1 (on the left) and L_2 (on the right).

We now show that L_1 are L_2 are decomposable by constructing, step by step, a parallel and sequential system containing then. First, consider the automaton $\mathcal{A}$ represented in Figure 8.9.

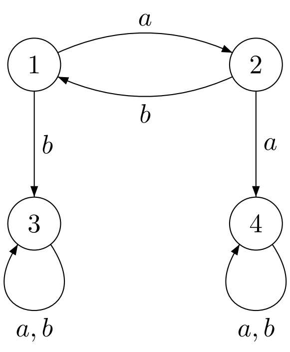


Figure 8.9: The automaton $\mathcal{A}$.

Let $L_{i,j}$ by the language of non-empty words accepted by $\mathcal{A}$ with i as initial state and j as the only final state. Let $L_{i,j,k}$ by the language of non-empty words accepted by $\mathcal{A}$ with i as initial state and j and k as final states. We are interested in the languages $L_{i,k}$ with $1 \leq i \leq 2$, $3 \leq k \leq 4$ and in the languages $L_{i,j,k}$ with $1 \leq i, j \leq 2$, $3 \leq k \leq 4$. These languages are $L_{1,3} = (ab)^*bA^*$, $L_{1,4} = (ab)^*aaA^*$, $L_{2,3} = (ba)^*bbA^*$, $L_{2,4} = (ba)^*aA^*$, $L_{1,1,3} = (ab)^+ \cup (ab)^*bA^* = L_1$,

$L_{1,1,4} = (ab)^+ \cup (ab)^*aaA^* = L_2$, $L_{1,2,3} = (ab)^*a \cup (ab)^*bA^*$, $L_{1,2,4} = (ab)^*a \cup (ab)^*aaA^*$, $L_{2,1,3} = (ba)^*b \cup L_{2,3} = (ba)^*bbA^*$, $L_{2,1,4} = (ba)^*b \cup (ba)^*aA^*$, $L_{2,2,3} = (ba)^+ \cup (ba)^*bbA^*$ and $L_{2,2,4} = (ba)^+ \cup (ba)^*aA^*$.

Let us calculate τ for these languages.

Proposition 8.1 *For $1 \leq i,j \leq 2$, $3 \leq k \leq 4$,*

$$\tau(L_{i,j,k}) = (\{1\} \times L_{i,j,k}) \cup (L_{i,k,j} \times \{1\}) \cup (L_{i,k} \times A^*) \bigcup_{1 \leq \ell \leq 2} (L_{i,\ell,k} \times L_{\ell,j,k})$$

Proof. If $(u,v) \in \tau(L_{i,j,k})$ for $1 \leq i,j \leq 2$ and $3 \leq k \leq 4$, then $uv \in L_{i,j}$ or $uv \in L_{i,k}$. It is clear that if $u = 1$ (resp. $v = 1$), then $(u,v) \in (\{1\} \times L_{i,j,k})$ (resp. $(u,v) \in L_{i,j,k} \times \{1\}$). So, from now on, we suppose that $u \neq 1$ and $v \neq 1$. If $uv \in L_{i,j}$, then $i \cdot uv = j$ in $\mathcal{A}$. Setting $\ell = i \cdot u$, we have $\ell \cdot v = j$ and since u and v are non-empty, $u \in L_{i,\ell} \subseteq L_{i,\ell,k}$ and $v \in L_{\ell,j} \subseteq L_{\ell,j,k}$. Furthermore, by the structure of the automaton $\mathcal{A}$, one can see that either $1 \leq \ell \leq 2$, or $uv \in L_{i,k}$. In the latter case, $i \cdot uv = k$. Since u and v are non-empty, by setting $\ell = i \cdot u$, we have $\ell \cdot v = k$. Then, we have two possibilities, $1 \leq \ell \leq 2$ or $\ell = k$. If $1 \leq \ell \leq 2$, then $u \in L_{i,\ell} \subseteq L_{i,j,\ell}$ and thus $v \in L_{\ell,k} \subseteq L_{\ell,j,k}$. On the other hand, if $\ell = k$, one has $u \in L_{i,k}$ and $v \in A^*$.

In the opposite direction, it is clear that if $(u,v) \in (\{1\} \times L_{i,j,k}) \cup (L_{i,j,k} \times \{1\})$, then $uv \in L_{i,j,k}$. If $(u,v) \in (L_{i,k} \times A^*)$ for $3 \leq k \leq 4$, then $i \cdot u = k$. Since $k \cdot v = k$, it follows that $i \cdot uv = k$, and thus $uv \in L_{i,k} \subseteq L_{i,j,k}$ for any $1 \leq j \leq 2$. Finally, if $(u,v) \in (L_{i,\ell,k} \times L_{\ell,j,k})$ for $1 \leq i,j,\ell \leq 2$ and $3 \leq k \leq 4$, then we have two possibilities $u \in L_{i,k}$ or $u \in L_{i,\ell}$. If $u \in L_{i,k}$, them $uv \in L_{i,j,k}$ since $(L_{i,k} \times A^*) \subseteq \tau(L)$. Otherwise, if $u \in L_{i,\ell}$, then $i \cdot u = \ell$ and since $v \in L_{\ell,j,k}$, $\ell \cdot v = j$ or $\ell \cdot v = k$, and so $i \cdot uv = j$ or $i \cdot uv = k$. In other words, $uv \in L_{i,j,k}$. $\square$

Proposition 8.2 *For $1 \leq i \leq 2$, $3 \leq k \leq 4$,*

$$\tau(L_{i,k}) = (\{1\} \times L_{i,k}) \cup (L_{i,k} \times A^*) \bigcup_{1 \leq \ell \leq 2} (L_{i,\ell,k} \times L_{\ell,k})$$

Proof. Suppose that $(u,v) \in \tau(L_{i,k})$ for $1 \leq i \leq 2$ and $3 \leq k \leq 4$, then $uv \in L_{i,k}$. It is clear that if $u = 1$, then $(u,v) \in (\{1\} \times L_{i,k})$. So, from now on, we suppose that $u \neq 1$. Since $uv \in L_{i,k}$, we have that $i \cdot uv = k$. Since u if not the empty word, by setting $\ell = i \cdot u$, we have that $\ell \cdot v = k$. Now, we have two possibilities, $1 \leq \ell \leq 2$ or $\ell = k$. If $1 \leq \ell \leq 2$, then $u \in L_{i,\ell} \subseteq L_{ilk}$ and thus $v \in L_{\ell,k}$. Otherwise if $\ell = k$, we have that $i \cdot u = k$, and so, for any $v \in A^*$, $i \cdot uv = k$, that is $v \in A^*$.

In the opposite direction, it is clear that if $(u,v) \in (\{1\} \times L_{i,j,k})$, then $uv \in L_{i,k}$. If $(u,v) \in (L_{i,k} \times A^*)$ for $3 \leq k \leq 4$, then $i \cdot u = k$, and since $k \cdot v = k$, it follows that $i \cdot uv = k$, and so $uv \in L_{i,k}$. Now, if $(u,v) \in (L_{i,\ell,k} \times L_{\ell,k})$ for $1 \leq i,j \leq 2$ and $3 \leq k \leq 4$, we have two possibilities $u \in L_{i,k}$ or $u \in L_{i,\ell}$. If $u \in L_{i,k}$ then $(u,v) \in \tau(L_{i,k})$. Finally, if $u \in L_{i,\ell}$ this implies that $i \cdot u = \ell$, and since $v \in L_{\ell,k}$, $\ell \cdot v = k$, that implies $i \cdot uv = k$ that is $uv \in L_{i,k}$. $\square$

Now, let us calculate σ for these languages.

Proposition 8.3

(1) $\sigma(L_{1,3}) = \sigma((ab)^*bA^*) = ((ab)^*bA^* \times A^*) \cup (A^* \times (ab)^*bA^*)$

(2) $\sigma(L_{2,4}) = \sigma((ba)^*aA^*) = ((ba)^*aA^* \times A^*) \cup (A^* \times (ba)^*aA^*)$

Proof. Let us prove (1). It is clear that if $(u, v) \in ((ab)^*bA^* \times A^*) \cup (A^* \times (ab)^*bA^*)$, then $(u \text{ Ш } v) \cap (ab)^*bA^* \neq \emptyset$. Now, suppose that $(u, v) \notin ((ab)^*bA^* \times A^*) \cup (A^* \times (ab)^*bA^*)$, that is, $u \notin (ab)^*bA^*$ and $v \notin (ab)^*bA^*$, then $u, v \in (ab)^* \cup (ab)^*a \cup (ab)^*aaA^*$. And since $\big((ab)^* \cup (ab)^*a \cup (ab)^*aaA^*\big) \text{ Ш } \big((ab)^* \cup (ab)^*a \cup (ab)^*aaA^*\big) = (ab)^* \cup (ab)^*a \cup (ab)^*aaA^*$, the result holds.

The proof for (2) is similar by swapping the letters a and b. $\square$

Proposition 8.4

(1)

$$\begin{aligned}\sigma(L_{14}) = \sigma((ab)^*aaA^*) =& ((ab)^*aaA^* \times A^*) \cup (A^* \times (ab)^*aaA^*) \\ & \cup ((ba)^*aA^* \times aA^*) \cup (aA^* \times (ba)^*aA^*)\end{aligned}$$

(2)

$$\begin{aligned}\sigma(L_{23}) = \sigma((ba)^*bbA^*) =& ((ba)^*bbA^* \times A^*) \cup (A^* \times (ba)^*bbA^*) \\ & \cup (bA^* \times (ab)^*bA^*) \cup ((ab)^*bA^* \times bA^*)\end{aligned}$$

Proof. Let us prove (1). It is clear that if $(u, v) \in ((ab)^*aaA^* \times A^*) \cup (A^* \times (ab)^*aaA^*)$, then $(u \text{ Ш } v) \cap (ab)^*aaA^* \neq \emptyset$. On the other hand, if $(u, v) \in (aA^* \times (ba)^*aA^*) \cup ((ba)^*aA^* \times aA^*)$, then $u = au'$ and $v = (ba)^n av'$ (resp. $u = (ba)^n au'$ and $u = au'$) for some $n \geq 0$, and then $a(ba)^n au'v' \in (ab)^*aaA^*$, that is $(u \text{ Ш } v) \cap (ab)^*aaA^* \neq \emptyset$. Now, suppose that $(u, v) \in \sigma((ab)^*aaA^*)$, this implies that there exists $w \in u \text{ Ш } v$ such that, $w \in (ab)^*aaA^*$. If $u = 1$ (resp. $v = 1$) then $(u, v) \in (A^* \times (ab)^*aaA^*)$ (resp. $(u, v) \in ((ab)^*aaA^* \times A^*)$). Then, suppose that $u \neq 1$ and $v \neq 1$. Now, if $u = bu'$ and $v = bv'$ for some $u', v' \in A^*$, $w = bw'$ for some $w' \in A^*$, and so $w \notin (ab)^*aaA^*$. Now, if $u = au'$ and $v = av'$ for some $u', v' \in A^*$, then $(u, v) \in (aA^* \times (ba)^*aA^*)$. Finally, suppose that $u = au'$ and $v = bv'$ for some $u', v' \in A^*$. If $u \in (ab)^*aaA^*$, then $(u, v) \in ((ab)^*aaA^* \times A^*)$, and if $v \in (ba)^+aA^*$, then $(u, v) \in (aA^* \times (ba)^*aA^*)$. So let us suppose that $u \notin (ab)^*aaA^*$ and $v \notin (ba)^*aA^*$. Then, necessarily $u \in (ab)^+ \cup (ab)^*a \cup (ab)^*bA^*$ and $v \in (ba)^+ \cup (ba)^*b \cup (ba)^*bbA^*$, and then since, $\Big(\big((ab)^+ \cup (ab)^*a \cup (ab)^*bA^*\big) \text{ Ш } \big((ba)^+ \cup (ba)^*b \cup (ba)^*bbA^*\big)\Big) \cap (ab)^*aaA^* = \emptyset$ the result holds. The proof for $u = bu'$ and $v = av'$ for some $u', v' \in A^*$ is similar.

The proof for (2) is similar but changing the letters a by b and b by a. $\square$

Proposition 8.5

(1) $\sigma(L_{1,1,3}) = \sigma((ab)^+ \cup (ab)^*bA^*) = \sigma((ab)^*bA^*) \cup (L_{1,1,3} \times L_{1,1,3})$

(2) $\sigma(L_{2,2,4}) = \sigma((ba)^+ \cup (ba)aA^*) = \sigma((ba)aA^*) \cup (L_{2,2,4} \times L_{2,2,4})$

Proof. Let us prove (1). If $(u,v) \in \sigma((ab)^*bA^*)$, then by definition $(u,v) \in \sigma((ab)^+ \cup (ab)^*bA^*)$. On the other hand if $(u,v) \in (L_{1,1,3} \times L_{1,1,3})$ we have two possibilities. If $u \in L_{1,3} = (ab)^*bA^*$ (resp. $v \in L_{1,3} = (ab)^*bA^*$) we know by Proposition 8.3 that $(u,v) \in \sigma(L_{1,3})$. Then, suppose that $(u,v) \in (ab)^+ \times (ab)^+$, this implies that $(u \text{ Ш } v) \cap (ab)^+ \neq \emptyset$, that is, $(u \text{ Ш } v) \cap L_{1,1,3} \neq \emptyset$, since $uv \in (ab)^+$.

In the opposite direction. Let $(u,v) \in \sigma(L_{1,1,3})$. If $(u \text{ Ш } v) \cap (ab)^*bA^* \neq \emptyset$, then the result holds by definition. So, let us suppose that $(u \text{ Ш } v) \cap (ab)^*bA^* = \emptyset$, then by Proposition 8.3, necessarily, $(u,v) \in \big((ab)^+ \cup (ab)^*a \cup (ab)^*aaA^*\big) \times \big((ab)^+ \cup (ab)^*a \cup (ab)^*aaA^*\big)$. Now, if $u \in (ab)^*aaA^*$ (resp.$v \in (ab)^*aaA^*$), then $(u \text{ Ш } v) \cap (ab)^+ = \emptyset$. So, suppose that $(u,v) \in (ab)^+ \cup (ab)^*a \times (ab)^+ \cup (ab)^*a$. If $u \in (ab)^*a$ (resp. $v \in (ab)^*a$), then for any $w \in u \text{ Ш } v$, $w \notin (ab)^+$ since the number of a's of w is greater than the number of b's of w. And so, $(u,v) \in (ab)^+ \times (ab)^+ \subseteq L_{1,1,3} \times L_{1,1,3}$.

The proof for (2) is similar. □

Proposition 8.6

(1)

$$\sigma(L_{1,2,3}) = \sigma((ab)^*a \cup (ab)^*bA^*) = \sigma((ab)^*bA^*) \cup (L_{1,1,3} \times L_{1,2,3}) \\ \cup (L_{1,2,3} \times L_{1,1,3})$$

(2)

$$\sigma(L_{2,1,4}) = \sigma((ba)^*b \cup (ba)^*aA^*) = \sigma((ba)^*aA^*) \cup (L_{2,2,4} \times L_{2,1,4}) \\ \cup (L_{2,1,4} \times L_{2,2,4})$$

Proof. Let us prove (1). If $(u,v) \in \sigma((ab)^*bA^*)$, then by definition $(u,v) \in \sigma((ab)^+ \cup (ab)^*bA^*)$. On the other hand if $(u,v) \in (L_{1,1,3} \times L_{1,2,3})$ (resp. $(u,v) \in (L_{1,1,3} \times L_{1,2,3})$) we have two possibilities. If $u \in L_{1,3} = (ab)^*bA^*$ (resp. $v \in L_{1,3} = (ab)^*bA^*$) we know by Proposition 8.3 that $(u,v) \in \sigma(L_{1,3})$. Then suppose that $(u,v) \in (ab)^+ \times (ab)^*a$ (resp.$(u,v) \in (ab)^*a \times (ab)^+$), since $uv \in (ab)^*a$, this implies that $(u \text{ Ш } v) \cap (ab)^*a \neq \emptyset$, and so, $(u \text{ Ш } v) \cap L_{1,2,4} \neq \emptyset$.

In the opposite direction. Let $(u,v) \in \sigma(L_{1,2,3})$. If $(u \text{ Ш } v) \cap (ab)^*bA^* \neq \emptyset$, then the result holds by definition. So, let us suppose that $(u \text{ Ш } v) \cap (ab)^*bA^* = \emptyset$, then by Proposition 8.3, necessarily, $(u,v) \in (ab)^+ \cup (ab)^*a \cup (ab)^*aaA^* \times (ab)^+ \cup (ab)^*a \cup (ab)^*aaA^*$. Now, if $u \in (ab)^*aaA^*$ (resp.$v \in (ab)^*aaA^*$), then $(u \text{ Ш } v) \cap (ab)^+ = \emptyset$. So, suppose that $(u,v) \in (ab)^+ \cup (ab)^*a \times (ab)^+ \cup (ab)^*a$. If $(u,v) \in ((ab)^+ \times (ab)^+)$ we have that for any $w \in u \text{ Ш } v$, $w \notin (ab)^*a$ since the number of a's of w is the same that the number of b's of w. If $(u,v) \in (ab)^*a \times (ab)^*a$ we have that for any $w \in u \text{ Ш } v$, $w \notin (ab)^*a$, since the number of a's of w is the same that the number of b's of w plus 2. And so, $(u,v) \in ((ab)^+ \times (ab)^*a) \cup ((ab)^*a \times ((ab)^+) \subseteq (L_{1,1,3} \times L_{1,2,3}) \cup (L_{1,2,3} \times L_{1,1,3})$.

The proof for (2) is similar. □

Proposition 8.7

(1)

$$\sigma(L_{1,2,4}) = \sigma((ab)^*a \cup (ab)^*aaA^*) = \sigma((ab)^*aaA^*) \cup (L_{1,2,4}) \times (L_{2,2,4}) \cup (L_{2,2,4}) \times (L_{1,2,4})$$

(2)

$$\sigma(L_{2,1,3}) = \sigma((ba)^*b \cup (ba)^*bbA^*) = \sigma((ba)^*bbA^*) \cup (L_{2,1,4}) \times (L_{1,1,4}) \cup (L_{1,1,4}) \times (L_{2,1,4})$$

Proof. Let us prove (1). If $(u,v) \in \sigma((ab)^*aaA^*)$, then by definition $(u,v) \in \sigma((ab)^+ \cup (ab)^*aaA^*)$. If $(u,v) \in (L_{1,2,4} \times L_{2,2,4})$ we have several possibilities. If $u \in L_{1,4} = (ab)^*aaA^*$ we know by Proposition 8.4 that $(u,v) \in \sigma(L_{1,4})$. If $v \in L_{2,4} = (ba)^*aA^*$, $v = (ba)^n av'$ for some $n \geq 0$ and some $v' \in A^*$, and since $u \in L_{1,2,4}$, $u = au'$ for some $u' \in A^*$, and so $a(ba)^n au'v' \in u \text{ Ш } v$. Then, suppose that $(u,v) \in (ab)^*a \times (ba)^+$, since $uv \in (ab)^*a$, we have that $(u \text{ Ш } v) \cap (ab)^*a \neq \emptyset$, that is, $(u \text{ Ш } v) \cap L_{1,2,3} \neq \emptyset$. Arguing in the same sense for $(L_{2,2,4}) \times (L_{1,2,4})$, we can suppose that $(u,v) \in (ba)^+ \times (ab)^*a \subseteq L_{2,2,4} \times L_{1,2,4}$, and then $vu \in (ab)^*a$.

In the opposite direction. Let $(u,v) \in \sigma(L_{1,2,4})$. If $(u,v) \in \sigma((ab)^*aaA^*)$, the result holds by definition. So, let us suppose that $(u \text{ Ш } v) \cap (ab)^*aaA^* = \emptyset$. This implies, by Proposition 8.4, that $(u,v) \in (aA^* \times bA^*) \cup (bA^* \times aA^*)$. Suppose that $(u,v) \in (aA^* \times bA^*)$, then, again by Proposition 8.4, we have that necessarily $u \in (ab)^+ \cup (ab)^*a \cup (ab)^*bA^*$ and $v \in (ba)^+ \cup b(ab)^* \cup (ba)^*bbA^*$. Now, if $u \in (ab)^*bA^*$ (resp. $v \in (ba)^*bbA^*$ and $v \in b(ab)^*$), then for any $w \in u \text{ Ш } v$ such that $w = aw'$ for some $w' \in A^*$, $w \in (ab)^+ \cup (ab)^*bA^*$, and so we can suppose that $(u,v) \in ((ab)^+ \cup (ab)^*a) \times (ba)^+$. If $(u,v) \in (ab)^+ \times (ba)^+$, then for any $w \in u \text{ Ш } v$, $w \notin L_{1,2,4}$ since if $w = aw'$ for some $w' \in A^*$, $w \in (ab)^+ \cup (ab)^*bA^*$. And so, $(u,v) \in ((ab)^*a \times (ba)^+) \subseteq (L_{1,2,4}) \times (L_{2,2,4})$. If we suppose that $(u,v) \in (bA^* \times aA^*)$, arguing in the same sense, we obtain the same result for $(u,v) \in ((ba)^+ \times (ab)^*a) \subseteq (L_{2,2,4}) \times (L_{1,2,4})$.

The proof for (2) is similar. □

Proposition 8.8

(1)

$$\sigma(L_{1,1,4}) = \sigma((ab)^+ \cup (ab)^*aaA^*) = \sigma((ab)^*aaA^*) \cup (L_{1,1,4}) \times (L_{2,2,4}) \cup (L_{1,2,4}) \times (L_{2,1,4}) \cup (L_{2,1,4}) \times (L_{1,2,4}) \cup (L_{2,2,4}) \times (L_{1,1,4})$$

(2)

$$\sigma(L_{2,2,3}) = \sigma((ba)^+ \cup (ba)^*bbA^*) = \sigma((ba)^*bbA^*) \cup (L_{1,1,4}) \times (L_{2,2,4}) \cup (L_{1,2,4}) \times (L_{2,1,4}) \cup (L_{2,1,4}) \times (L_{1,2,4}) \cup (L_{2,2,4}) \times (L_{1,1,4})$$

Proof.

Let us prove (1). If $(u,v) \in \sigma((ab)^*aaA^*)$, then by definition $(u,v) \in \sigma((ab)^+ \cup (ab)^*aaA^*)$. If $(u,v) \in (L_{1,1,4} \times L_{2,2,4})$ we have several possibilities, if $u \in L_{1,4} = (ab)^*aaA^*$ we know by Proposition 8.4 that $(u,v) \in \sigma(L_{1,4})$.

If $v \in L_{2,4} = (ba)^*aA^*$, $v = (ba)^n av'$ for some $n \geq 0$ and some $v' \in A^*$, and since $u \in L_{1,1,4}$, $u = au'$ for some $u' \in A^*$, and so $a(ba)^n auv' \in u$ Ш v. Then, suppose that $(u, v) \in (ab)^+ \times (ba)^+$, then $u = (ab)^n$ and $v = (ba)^m$ for some $n, m > 0$, then $a(ba)^m b(ab)^{n-1} \in (ab)^+$, and so $(u$ Ш $v) \cap (ab)^+ \neq \emptyset$, that is, $(u$ Ш $v) \cap L_{1,2,4} \neq \emptyset$. Arguing in the same sense for $(L_{2,2,4}) \times (L_{1,1,4})$, we can suppose that $(u, v) \in (ba)^+ \times (ab)^+$, and then $(u$ Ш $v) \cap (ab)^+ \neq \emptyset$.

If $(u, v) \in (L_{1,2,4} \times L_{2,1,4})$, there ave several possibilities. If $u \in L_{1,4} = (ab)^*aaA^*$, we know by Proposition 8.4 that $(u, v) \in \sigma(L_{1,4})$. If $v \in L_{2,4} = (ba)^*aA^*$, $v = (ba)^n av'$ for some $n \geq 0$ and some $v' \in A^*$, and since $u \in L_{1,2,4}$, $u = au'$ for some $u' \in A^*$, and so $a(ba)^n au'v' \in u$ Ш v. Then, suppose that $(u, v) \in (ab)^*a \times (ba)^*b$, then $uv \in (ab)^+$, and so $(u$ Ш $v) \cap (ab)^+ \neq \emptyset$,that is, $(u$ Ш $v) \cap L_{1,2,4} \neq \emptyset$. Arguing in the same sense for $(L_{2,1,4}) \times (L_{1,2,4})$, we can suppose that $(u, v) \in (ba)^*b \times (ab)^*a$, and then $(u$ Ш $v) \cap (ab)^+ \neq \emptyset$, since $vu \in (ab)^+$, that is, $(u$ Ш $v) \cap (L_{1,1,4}) \neq \emptyset$.

In the opposite direction. Let $(u, v) \in \sigma(L_{1,2,4})$. If $(u, v) \in \sigma((ab)^*aaA^*)$, the result holds by definition. So, let us suppose that $(u$ Ш $v) \cap (ab)^*aaA^* = \emptyset$. This implies, by Proposition 8.4, that $(u, v) \in (aA^* \times bA^*) \cup (bA^* \times aA^*)$. Suppose that $(u, v) \in (aA^* \times bA^*)$, then, again by Proposition 8.4, we have that necessarily $u \in (ab)^+ \cup (ab)^*a \cup (ab)^*bA^*$ and $v \in (ba)^+ \cup b(ab)^* \cup (ba)^*bbA^*$. Now, if $u \in (ab)^*bA^*$ (resp. $v \in (ba)^*bbA^*$), then for any $w \in u$ Ш v such that $w = aw'$ for some $w' \in A^*$, $w \in (ab)^*bA^*$, and so we can suppose that $(u, v) \in ((ab)^+ \cup (ab)^*a) \times ((ba)^+ \cup (ba)^*b)$. If $(u, v) \in (ab)^+ \times (ba)^*b$ (resp. $(u, v) \in (ab)^*a \times (ba)^+$), then $(u$ Ш $v) \cap (ab)^* = \emptyset$. And so, $(u, v) \in (ab)^+ \times (ba)^+ \cup (ab)^*a \times (ba)^*a \subseteq L_{1,1,4} \times L_{2,2,4} \cup L_{1,2,4} \times L_{2,1,4}$. A similar argument can by used to show that if $(u, v) \in bA^* \times aA^*$ with $(u$ Ш $v) \cap (ab)^*aaA^* = \emptyset$, then $(u, v) \in (ba)^+ \times (ab)^+ \cup (ba)^*b \times (ab)^*a \subseteq L_{2,2,4} \times L_{1,1,4} \cup L_{2,1,4} \times L_{1,2,4}$.

The proof for (2) is similar. $\square$

We are now ready to show that L_1 and L_2 are not decomposable. By Theorem 4.6, all languages which are products of commutative languages are decomposable. In particular, the following languages are decomposable: aA^* and bA^*.

Theorem 8.9 *The languages L_1 and L_2 are decomposable.*

Proof. Let us define a system $\mathcal{S}$ consisting of the unions of the languages: $L_{i,j,k}$ for $1 \leq i, j \leq 2$ and $3 \leq k \leq 4$, $\{1\}$, A^* and the languages of the systems $\mathcal{S}(aA^*)$ and $\mathcal{S}(bA^*)$. Note that L_1 and L_2 belong to $\mathcal{S}$ since $L_1 = L_{1,1,3}$ and $L_2 = L_{1,1,4}$. It remains to show that for any language L' of S $\tau(L')$ and $\sigma(L')$ can be obtained as the union of languages $(M \times N)$ where M and N belong to $\mathcal{S}$. For the languages $L_{i,j,k}$ and $L_{i,k}$ with $1 \leq i, j \leq 2$ and $3 \leq k \leq 4$, the result follows from Propositions 8.1, 8.2, 8.3, 8.4 8.5, 8.6, 8.7 and 8.8. Clearly, $\tau(\{1\}) = \sigma(\{1\}) = (\{1\} \times \{1\})$ and $\tau(A^*) = \sigma(A^*) = (A^* \times A^*)$. For any language of the systems described above, its image under τ and σ can be obtained from the languages of these systems, because they are parallel and sequential systems. Finally, since for any languages N_1 and N_2, the formulas $\tau(N_1 \cup N_2) = \tau(N_1) \cup \tau(N_2)$ and $\sigma(N_1 \cup N_2) = \sigma(N_1) \cup \sigma(N_2)$ hold, the system $\mathcal{S}$ is a parallel and sequential system. $\square$

Proposition 8.10 *Decomposable languages are not closed under intersection.*

Proof. We know by Theorem 8.9 that the languages of the previous section $L_1 = (ab)^+ \cup (ab)^*bA^*$ and $L_2 = (ab)^+ \cup (ab)^*aaA^*$ are decomposable, but we know that by Proposition 3.4 that $L_1 \cap L_2 = (ab)^+$ is not. $\square$

9 More on group languages

Let G be a finite group, let $\pi : A^* \to G$ be a surjective morphism and let $L = \pi^{-1}(1)$. A well-known result states that sufficiently long words contain a factor in L. More precisely

Lemma 9.1 *Every word of A^* of length $\geq |G|$ contains a non-empty factor in L.*

Proof. Let $a_1 \cdots a_n$ be a word of length $n \geq |G|$. Consider the sequence $1, \pi(a_1), \pi(a_1a_2), \ldots, \pi(a_1a_2 \cdots a_n)$. This sequence of length $n+1$ necessarily contains two equal terms, say $\pi(a_1 \cdots a_i) = \pi(a_1 \cdots a_j)$ with $j > i$. It follows, since G is a group, that $\pi(a_{i+1} \cdots a_j) = 1$. Therefore $a_{i+1} \cdots a_j \in L$. $\square$

Proposition 9.2 *If the language L is decomposable, then every language recognized by π is recognizable.*

Proof. Let P be a subset of G. Since decomposable languages are closed union and since

$$\pi^{-1}(P) = \bigcup_{g \in P} \pi^{-1}(g)$$

it suffices to prove that each language $\pi^{-1}(g)$ is decomposable. Now, let g be a fixed element of G and let u be a word such that $\pi(u) = g^{-1}$. We claim that $\pi^{-1}(g) = Lu^{-1}$. Indeed if $x \in \pi^{-1}(g)$, then $\pi(xu) = \pi(x)\pi(u) = gg^{-1} = 1$. It follows that $xu \in L$ and $x \in Lu^{-1}$. Conversely, if $x \in Lu^{-1}$, then $xu \in L$, that is, $\pi(xu) = 1$. Therefore $\pi(x) = \pi(u)^{-1} = g$ and $x \in \pi^{-1}(g)$, which proves the claim. Now, Proposition 4.4 shows that decomposable languages are closed under quotients, and thus $\pi^{-1}(g)$ is decomposable. $\square$

We first give an explicit formula for $\sigma(L)$.

Proposition 9.3 *The following formula holds, with $N = |G|^4$:*

$$\sigma(L) = \bigcup_{\substack{r,s \leq N \\ (a_1 \cdots a_r \,Ш\, b_1 \cdots b_s) \cap L \neq \emptyset}} (La_1La_2L \cdots La_rL) \;Ш\; (Lb_1Lb_2L \cdots Lb_sL)$$

Proof. Let $a_1 \cdots a_r$ and $b_1 \cdots b_s$ be two words such that $r, s \leq N$ and

$$(a_1 \cdots a_r \;Ш\; b_1 \cdots b_s) \cap L \neq \emptyset$$

Then there exists in L a word w of length $r+s$ and a partition (I, J) of $\{1, \cdots, r+s\}$ such that $w[I] = a_1 \cdots a_r$ and $w[J] = b_1 \cdots b_s$ (if $I = \{i_1, i_2, \ldots, i_k\}$, then $w[I]$ denotes the word $a_{i_1} \cdots a_{i_k}$).

Suppose that $(u, v) \in (La_1La_2L \cdots La_rL) \;Ш\; (Lb_1Lb_2L \cdots Lb_sL)$. Then $u = u_0a_1u_1 \cdots a_ru_r$ and $v = v_0b_1v_1 \cdots b_sv_s$ for some words $u_0, u_1, \ldots, u_r, v_0, \ldots, v_r \in L$.

References

[1] J. Baeten and W. Weijland, *Process algebra*, *Cambridge Tract in Theoretical Computer Science* vol. 18, Cambridge University Press, Cambridge UK, 1990.

[2] S. Eilenberg, *Automata, Languages and Machines*, vol. B, Academic Press, New York, 1976.

[3] Lothaire, *Combinatorics on Words*, *Encyclopedia of Mathematics and its Applications* vol. 17, aw, reading, 1983.

[4] J.-E. Pin and P. Weil, Polynomial closure and unambiguous product, journal = Theory Comput. Systems, year = 1997, volume = 30, pages = 1–39,.

[5] P. Schnoebelen, Decomposable regular languages and the shuffle operator, *EATCS Bull.* ,67 (1999), 283–289.